Norton AntiVirus™ User's Guide

Norton AntiVirus™ 2002

Norton AntiVirus™ User's Guide

Documentation version 8.0

PN: 07-30-00469

Copyright Notice

Trademarks

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

SYMANTEC LICENSE AND WARRANTY

IMPORTANT: PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND SYMANTEC. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK ON THE "I DO NOT AGREE", "NO" BUTTON, OR OTHERWISE INDICATE REFUSAL, MAKE NO FURTHER USE OF THE SOFTWARE, AND RETURN THE FULL PRODUCT WITH PROOF OF PURCHASE TO THE DEALER FROM WHOM IT WAS ACQUIRED WITHIN SIXTY (60) DAYS OF PURCHASE, AND YOUR MONEY WILL BE REFUNDED.

1. License.

The software which accompanies this license (collectively the "Software") is the property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, you will have certain rights to use the Software after your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that Symantec may furnish to you. Except as may be modified by a Symantec license certificate, license coupon, or license key (each a "License Module") which accompanies, precedes, or follows this license, your rights and obligations with respect to the use of this Software are as follows:

You may:

A. use one copy of the Software on a single computer. If a License Module accompanies, precedes, or follows this license, you may make that number of copies of the Software licensed to you by Symantec as provided in your License Module. Your License Module shall constitute proof of your right to make such copies.

B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of your computer and retain the original for archival purposes;

C. use the Software on a network, provided that you have a licensed copy of the Software for each computer that can access the Software over that network; and

D. after written notice to Symantec, transfer the Software on a permanent basis to another person or entity, provided that you retain no copies of the Software and the transferee agrees to the terms of this license.

You may not:

A. copy the printed documentation which accompanies the Software;

B. sublicense, rent or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;

C. use a previous version or copy of the Software after you have received a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;

D. use a later version of the Software than is provided herewith unless you have purchased upgrade insurance or have otherwise separately acquired the right to use such later version;

E. use, if you received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which you have not received a permission in a License Module; or

F. use the Software in any manner not authorized by this license.

2. Content Updates:

Certain Symantec software products utilize content that is updated from time to time (antivirus products utilize updated virus definitions; content filtering products utilize updated URL lists; firewall products utilize updated firewall rules; vulnerability assessment products utilize updated vulnerability data, etc.; collectively, these are referred to as "Content Updates"). You may obtain Content Updates for any period for which you have purchased a subscription for Content Updates for the Software (including any subscription included with your original purchase of the Software), purchased upgrade insurance for the Software, entered into a maintenance agreement that includes Content Updates, or otherwise separately acquired the right to obtain Content Updates. This license does not otherwise permit you to obtain and use Content Updates.

3. Sixty Day Money Back Guarantee:

If you are the original licensee of this copy of the Software and are dissatisfied with it for any reason, you may return the complete product, together with your receipt, to Symantec or an authorized dealer, postage prepaid, for a full refund at any time during the sixty (60) day period following the delivery to you of the Software.

4. Limited Warranty:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to you. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money you paid for the Software. Symantec does not warrant that the Software will meet your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

5. Disclaimer of Damages:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR

INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC OR ITS LICENSORS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S OR ITS LICENSORS' LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether you accept the Software.

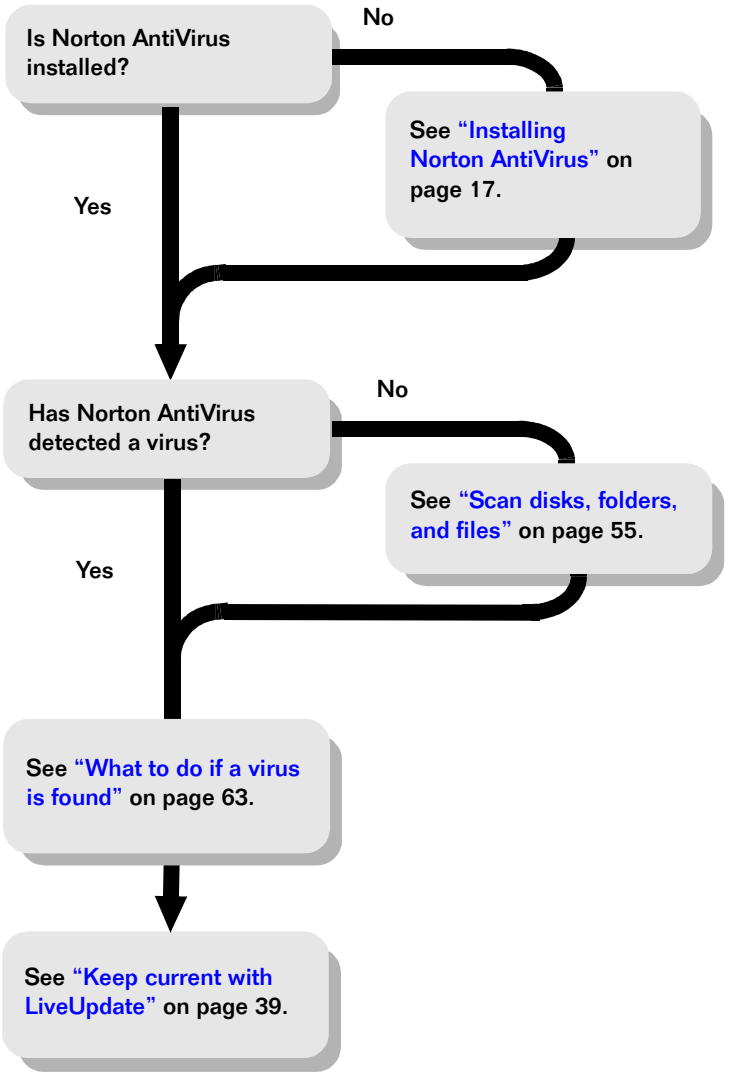
6. U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items", as that term is defined in 48 C.F.R. section 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation", as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

7. General:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment or similar communications between the parties. This Agreement may only be modified by a License Module or by a written document which has been signed by both You and Symantec. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. Should you have any questions concerning this Agreement, or if you desire to contact Symantec for any reason, please write: (i) Symantec Customer Service, 175 W. Broadway, Eugene, OR 97401, USA, or (ii) Symantec Customer Service Center, PO BOX 5689, Dublin 15, Ireland.

What to do if a virus is found



C O N T E N T S

Chapter 3 Norton AntiVirus basics

Chapter 4 Protecting disks, files, and data from viruses

CHAPTER 1

About Norton AntiVirus

Norton AntiVirus provides comprehensive virus prevention, detection, and elimination software for your computer. It finds and repairs infected files to keep your data safe and secure. Easy updating of the virus definition service over the Internet keeps Norton AntiVirus prepared for the latest threats.

What's new in Norton AntiVirus

Norton AntiVirus 2002 introduces access to Norton AntiVirus tools through Windows Explorer, more extensive email support, increased automation of virus repair with improved nonobtrusive feedback, and Windows XP support.

- Norton AntiVirus tools in Windows Explorer: For users with Internet Explorer 5.0 or higher and for Windows NT users with the Windows Desktop Update, Norton AntiVirus 2002 adds a button to the Windows Explorer toolbar that allows you to view protection status, manage the Quarantine area of your computer, view the Activity Log, view the virus encyclopedia, and scan for viruses.
- Expanded email protection: Norton AntiVirus now supports email programs that use POP3 and SMTP communications protocols without having to change the email program's configuration. You can choose to scan both incoming and outgoing emails.
- Automated virus repair: Norton AntiVirus can scan and repair your files entirely in the background, requiring no intervention from you. You receive a report containing the results of the scan.
- Norton AntiVirus provides complete anti-virus protection for your Windows XP operating system.

How viruses work

A *computer virus* is a parasitic program written intentionally to alter the way your computer operates without your permission or knowledge. A virus attaches copies of itself to other files and, when activated, may damage files, cause erratic system behavior, or display messages.

Computer viruses infect system files and documents created by programs with macro capabilities. Some system viruses are programmed specifically to corrupt programs, delete files, or erase your disk.

Macro viruses spread quickly

Macros are simple programs that are used to do things such as automate repetitive tasks in a document or make calculations in a spreadsheet. Macros are written in files created by such programs as Microsoft Word and Microsoft Excel.

Macro viruses are malicious macro programs that are designed to replicate themselves from file to file and can often destroy or change data. Macro viruses can be transferred across platforms and spread whenever you open an infected file.

Trojan horses hide their true purposes

Trojan horses are programs that appear to serve some useful purpose or provide entertainment, which encourages you to run them. But the program also serves a covert purpose, which may be to damage files or place a virus on your computer.

A Trojan horse is not a virus because it does not replicate and spread like a virus. Because Trojan horses are not viruses, files that contain them cannot be repaired. To ensure the safety of your computer, Norton AntiVirus detects Trojan horses so you can delete them from your computer.

Worms take up space

Worms are programs that replicate without infecting other programs. Some worms spread by copying themselves from disk to disk. They search for specific types of files on a hard disk or server volume, and try to damage or destroy those files. Other worms replicate only in memory, creating myriad copies of themselves, all running simultaneously, which slows down the computer. Like Trojan horses, worms are not viruses and therefore cannot be repaired. They must be deleted from your computer.

How viruses spread

A virus is inactive until you launch an infected program, start your computer from a disk that has infected system files, or open an infected document. For example, if a word processing program contains a virus, the virus activates when you run the program. Once a virus is in memory, it usually infects any program you run, including network programs (if you can make changes to network folders or disks).

Viruses behave in different ways. Some viruses stay active in memory until you turn off your computer. Other viruses stay active only as long as the infected program is running. Turning off your computer or exiting the program removes the virus from memory, but does not remove the virus from the infected file or disk. That is, if the virus resides in an operating system file, the virus activates the next time you start your computer from the infected disk. If the virus resides in a program, the virus activates the next time you run the program.

To prevent virus-infected programs from getting onto your computer, scan files with Norton AntiVirus before you copy or run them. This includes programs you download from news groups or Internet Web sites and any email attachments that you receive.

How Norton AntiVirus works

Norton AntiVirus monitors your computer for known and unknown viruses. A *known virus* is one that can be detected and identified by name. An *unknown virus* is one for which Norton AntiVirus does not yet have a definition.

Norton AntiVirus protects your computer from both types of viruses, using virus definitions to detect known viruses, and Bloodhound technology and Script Blocking to detect unknown viruses. Virus definitions, Bloodhound technology, and Script Blocking are all used during scheduled scans and manual scans, and are used by Auto-Protect to constantly monitor your computer.

The virus definition service stops known viruses

The *virus definition service* consists of files that Norton AntiVirus uses to recognize viruses and intercept their activity. You can look up virus names in Norton AntiVirus, and access an encyclopedia of virus descriptions on the Symantec Web site. For more information, see "Look up virus names and definitions" on page 72.

Bloodhound technology stops unknown viruses

Bloodhound is the Norton AntiVirus scanning technology for detecting new and unknown viruses. It detects viruses by analyzing an executable file's structure, behavior, and other attributes such as programming logic, computer instructions, and any data contained in the file. It also sets up simulated environments in which to load documents and test for macro viruses.

Script Blocking stops script-based viruses

A *script* is a list of instructions that can be executed without user interaction. Scripts can be opened with text editors or word processing programs, so they are very easy to change.

Script Blocking detects Visual Basic and Java script-based viruses without the need for specific virus definitions. It monitors the scripts for virus-like behavior and alerts you if it is found.

Auto-Protect keeps you safe

Norton AntiVirus Auto-Protect loads into memory when Windows starts, providing constant protection while you work.

Using Auto-Protect, Norton AntiVirus automatically:

- Eliminates viruses and Trojan horses, including macro viruses, and repairs damaged files
- Checks for viruses every time you use software programs on your computer, insert floppy disks or other removable media, or use document files that you receive or create
- Monitors your computer for any unusual symptoms that may indicate an active virus
- Protects your computer from Internet-borne viruses

How to maintain protection

When Norton AntiVirus is installed, you have complete virus protection. However, new viruses are created constantly. Viruses can spread when you start your computer from an infected disk or when you run an infected program. There are several things you can to do avoid viruses and to recover quickly should a virus strike.

Avoid viruses

It is important that you practice regular file maintenance and that you keep Norton AntiVirus up-to-date.

To avoid viruses:

- Write-protect removable media.
- Stay informed about viruses by logging on to the Symantec Security Response Web site (securityresponse.symantec.com) where there is extensive, frequently updated information on viruses and virus protection.
- Use LiveUpdate regularly to update your programs and virus definition service files. For more information, see "Keep current with LiveUpdate" on page 39.
- Keep Norton AntiVirus Auto-Protect turned on at all times to prevent viruses from infecting your computer.

- If Norton AntiVirus Auto-Protect is not turned on, scan removable media before you use them. For more information, see "Scan disks, folders, and files" on page 55.
- Schedule scans to occur automatically. For more information, see "Schedule automatic virus scans" on page 60.

Prepare for emergencies

It is also important that you are prepared in case your computer is infected by a virus.

To prepare for emergencies:

- Back up files regularly and keep more than just the most recent backup.
- If you are using Windows NT, Windows 2000, or Windows XP and your computer cannot start from a CD, create a set of Emergency Disks, from which you can start your computer and scan for viruses. For more information, see "Create Emergency Disks" on page 19.
- If you are using Windows 98 or Me, create a set of Rescue Disks, with which you can start your computer in DOS mode and use Norton AntiVirus to fix virus-related problems and recover from a system crash. For more information, see "About Rescue Disks" on page 34.

CHAPTER 2

Installing Norton AntiVirus

Before installing Norton AntiVirus, take a moment to review the system requirements listed in this chapter. Windows 98 and Windows Me users should have some blank 1.44 MB disks available to make Rescue Disks.

System requirements

To use Norton AntiVirus, your computer must have one of the following Windows operating systems:

- Windows 98, 98SE
- Windows Me
- Windows NT 4.0 Workstation with service pack 6 or higher
- Windows 2000 Professional
- Windows XP Professional or Windows XP Home Edition

Your computer must also meet the following minimum requirements.

Windows 98/Me

- Intel Pentium processor at 133MHz for Windows 98; 150 MHz for Windows Me
- 32 MB of RAM
- 50 MB of available hard disk space
- Internet Explorer 4.01 service pack 1 or higher
- CD-ROM or DVD-ROM drive

Windows NT 4.0 Workstation

- Service pack 6 or higher
- Intel Pentium processor at 133MHz or higher
- 32 MB of RAM
- 50 MB of available hard disk space
- Internet Explorer 4.01 service pack 1 or higher
- CD-ROM or DVD-ROM drive

Windows 2000 Professional

- Intel Pentium processor at 133MHz or higher
- 64 MB of RAM
- 50 MB of hard disk space
- Internet Explorer 4.01 service pack 1 or higher
- CD-ROM or DVD-ROM drive

Windows XP Home Edition/Professional

- Intel Pentium processor at 300MHz or higher
- 128 MB of RAM
- 50 MB of hard disk space
- Internet Explorer 4.01 service pack 1 or higher
- CD-ROM or DVD-ROM drive

Before installation

Before you install Norton AntiVirus, prepare your computer. If your computer cannot start from a CD, create Emergency Disks.

Prepare your computer

If you have a previous version of Norton AntiVirus or any other anti-virus programs on your computer, you must uninstall them before installing Norton AntiVirus. For more information, see "If you need to uninstall Norton AntiVirus" on page 27.

To uninstall other anti-virus programs, see the user documentation that came with the program.

You must close all other Windows programs before installing Norton AntiVirus.

Create Emergency Disks

Emergency Disks are used to start your computer and scan for viruses in case of a problem. If your computer can start from a CD, you can use the Norton AntiVirus CD in place of Emergency Disks and do not need to create them. If you cannot start your computer, you can use these instructions to create Emergency Disks on another computer. For more information, see "If you need to use Emergency Disks" on page 71.

Use the Norton AntiVirus CD to create Emergency Disks. You will need several formatted 1.44 MB disks.

To create Emergency Disks

1. Insert the Norton AntiVirus CD into the CD-ROM drive.
2. Click **Browse CD**.
3. Double-click the **Support** folder.
4. Double-click the **Edisk** folder.
5. Double-click **Ned.exe**.
6. In the welcome window, click **OK**.
7. Label the first disk as instructed and insert it into drive A.
8. Click **Yes**.
9. Repeat steps 7 and 8 for the subsequent disks.
10. When the procedure is complete, click **OK**.
11. Remove the final disk from drive A and store the Emergency Disk set in a safe place.

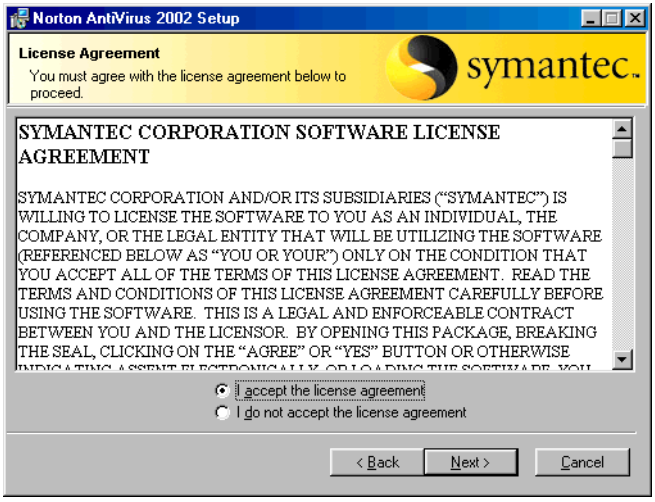
Install Norton AntiVirus

Install Norton AntiVirus from the Norton AntiVirus CD.

To install Norton AntiVirus

1. Insert the Norton AntiVirus CD into the CD-ROM drive.
2. In the Norton AntiVirus 2002 window, click **Install Norton AntiVirus**.

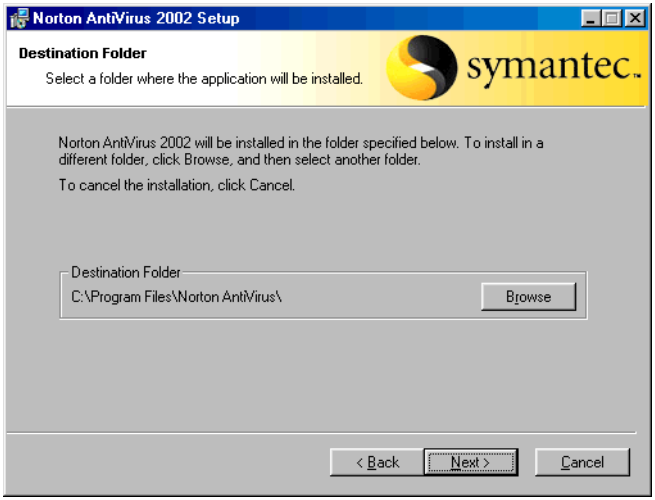
   If your computer is not set to automatically open a CD, you will have to open it yourself. For more information, see "If the opening screen does not appear" on page 23.
3. If you are installing in Windows 98, 98SE, or Me, Norton AntiVirus scans your computer's memory for viruses before installing. If a virus is found, you are prompted to use your Emergency Disks to remove the virus before continuing. For more information, see "If you need to use Emergency Disks" on page 71.
4. The opening installation window reminds you to close all other Windows programs. Click **Next**.



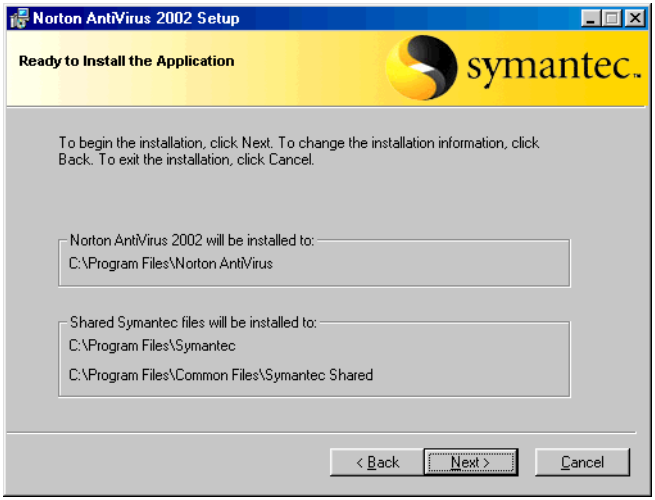
5. In the License Agreement window, click **I accept the license agreement**.

   If you decline, you cannot continue with the installation.

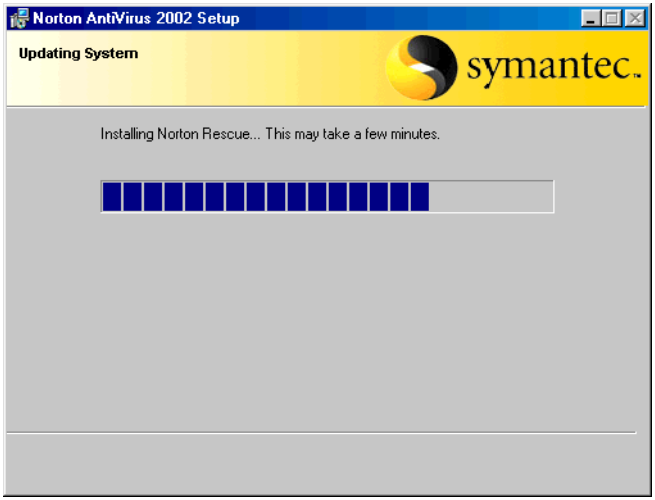
6 Click **Next**.



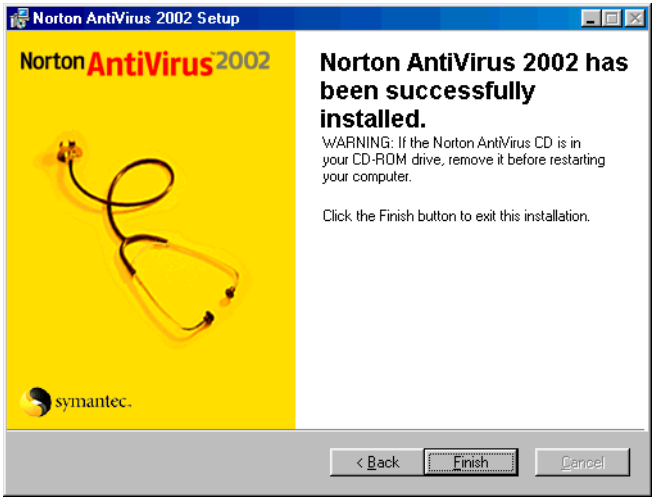
7 Select a folder into which you want to install Norton AntiVirus, then click **Next**.



8 Confirm the installation location, then click **Next**.



9 After Norton AntiVirus is installed, scroll through the Readme text, then click **Next**.



10 Click **Finish** to exit the installation.

If the opening screen does not appear

Sometimes, a computer's CD-ROM drive does not automatically start a CD.

To start the installation from the Norton AntiVirus CD

1. On your desktop, double-click **My Computer**.
2. In the My Computer dialog box, double-click the icon for your CD-ROM drive.
3. From the list of files, double-click **CDSTART.EXE**.

After installation

If your computer needs to be restarted after Norton AntiVirus is installed, a prompt appears giving you the option to do so immediately. After restart or, if your computer does not need to be restarted, after installation is complete, the Information Wizard appears.

Note: If you bought your computer with Norton AntiVirus already installed, the Information Wizard appears the first time you start Norton AntiVirus. You must accept the license agreement that appears in the Information Wizard for Norton AntiVirus to be activated.

Restart your computer

After installation, you may receive a prompt telling you that your computer needs to be restarted for the updates to take effect.

To restart your computer

- In the dialog box, click **Yes**.

  If you click No, configuration of Norton AntiVirus is not complete until you restart your computer.

Use the Information Wizard

The Information Wizard lets you register your copy of Norton AntiVirus, get information about the virus protection subscription service, select post-install tasks to be done automatically, and review your Norton AntiVirus settings. If you do not complete the Information Wizard, Norton AntiVirus uses the default settings for post-install tasks and program options.

Note: If you choose not to register the software using the Information Wizard or if registration fails for some reason, you can register on the Symantec Web site at www.symantec.com or by using the Product Registration option on the Help menu. On the Web site, go to the Products page for the registration link.

To use the Information Wizard

1. In the welcome window, click **Next**.

   If you purchased your computer with Norton AntiVirus already installed, you must accept the license agreement in order to use Norton AntiVirus.
2. Click **I accept the license agreement**, then click **Next**.
3. In the first Registration window, select the country from which you are registering and the country in which you live (if different), then click **Next**.
4. If you would like information from Symantec about Norton AntiVirus, select the method by which you want to receive that information, then click **Next**.
5. Enter your name and whether you want Norton AntiVirus registered to you or your company, then click **Next**.
6. Enter your address, then click **Next**.
7. Answer the survey questions to help Symantec improve its products and services, then click **Next** when you are done or to skip the survey.
8. Select whether you want to register Norton AntiVirus through the Internet or by mail, then click **Next**.

   If you submitted your registration through the Internet, a dialog box displays the serial number for your product.
9. Write down the number or click **Print** to get a copy of your registration information for future reference.

10 Click **Next**.

11 Select whether you want to use your existing profile the next time you register a Symantec product, or type the information as part of registration.

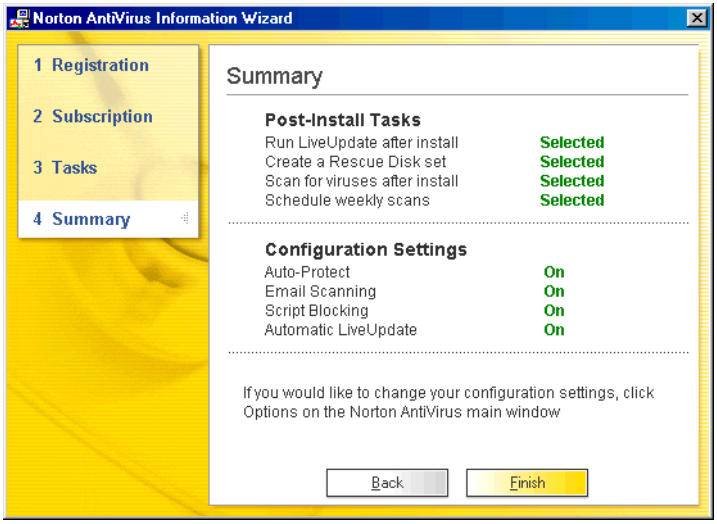
12 Click **Finish**.

13 Review the subscription service information, then click **Next**.

14 Select the post-install tasks that you want Norton AntiVirus to perform automatically. Your options are:

- Run LiveUpdate to ensure that you have the latest virus definitions. For more information, see "Keep current with LiveUpdate" on page 39.
- Perform a full system scan. For more information, see "Scan disks, folders, and files" on page 55.
- Schedule a weekly scan of your local hard drives. You must have Microsoft Scheduler installed to use this option. If you select this option, you can change the schedule for this scan as desired. For more information, see "Schedule automatic virus scans" on page 60.
- If you are installing in Windows 98 or Windows Me, you also have the option to create a Rescue Disk set. For more information, see "About Rescue Disks" on page 34.

15 Click **Next**.



16 Review the configuration settings for Norton AntiVirus. If you want to change any of the settings, do so using Norton AntiVirus Options. For more information, see "Customize Norton AntiVirus" on page 43.

17 Click **Finish**.

If you selected any post-install tasks, they start automatically.

Read the Readme file

The Readme file contains technical tips and information about product changes that occurred after this guide went to press. It is installed on your hard disk in the same location as the Norton AntiVirus product files.

To read the Readme file

1 Using Windows Explorer, navigate to the location where your Norton AntiVirus files are installed.

If you installed Norton AntiVirus in the default location, the files are in C:\Program Files\Norton AntiVirus.

2 Double-click **Readme.txt** to open the file in Notepad or WordPad.

The Readme file includes instructions for printing it if you want to do so.

3 Close the word processing program when you are done reading the file.

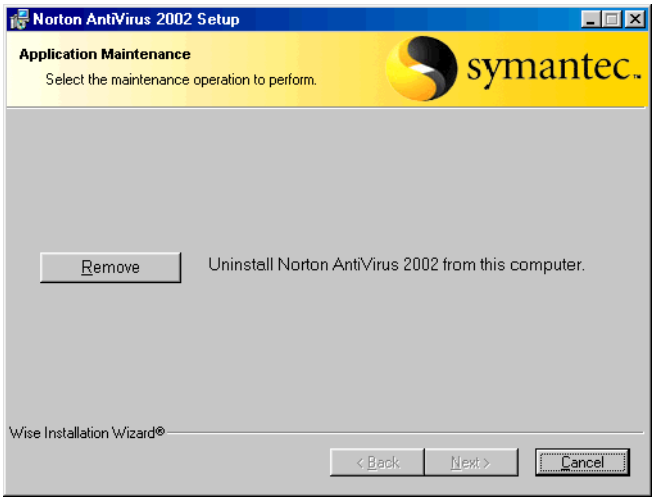
If you need to uninstall Norton AntiVirus

If you need to remove Norton AntiVirus from your computer, use the Uninstall Norton AntiVirus option on the Windows Start menu.

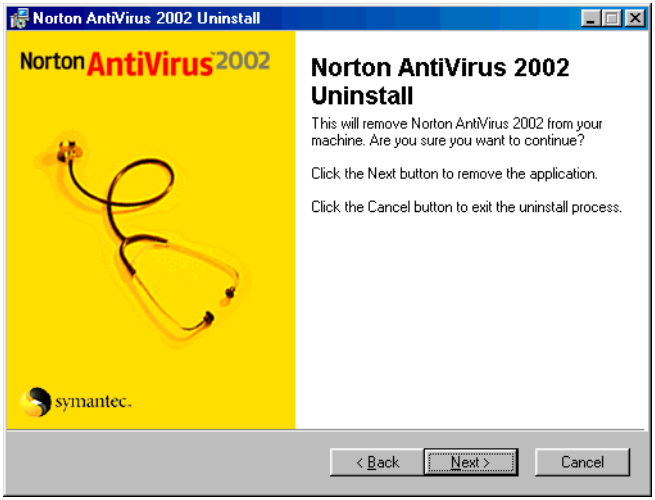
Note: During uninstall, Windows may indicate that it is installing software. This is a standard Microsoft installation message and can be disregarded.

To uninstall Norton AntiVirus

1 On the Windows taskbar, click **Start > Programs > Norton AntiVirus > Uninstall Norton AntiVirus**.



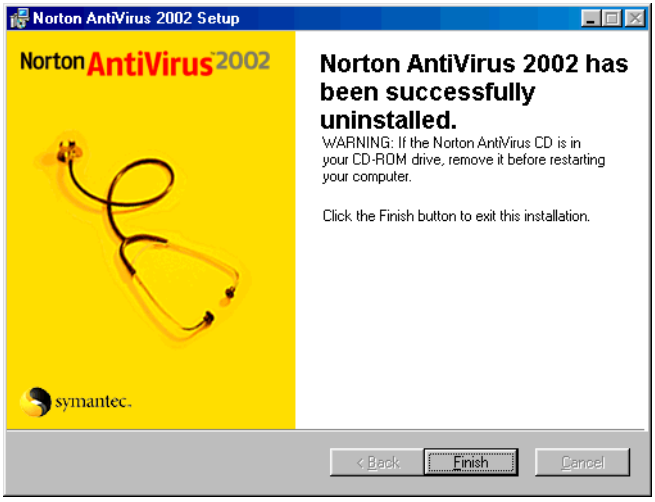
2 Click **Remove** to confirm that you want to uninstall the product.



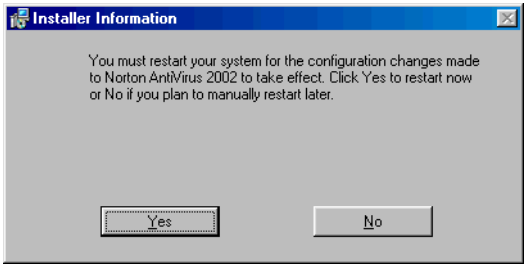
3 Click **Next**.

4 If you have files in Quarantine, you are asked if you want to delete them. Select one of the following:

- Yes: Deletes the quarantined files from your computer.
- No: Leaves the quarantined files on your computer, but makes them inaccessible. To repair or submit the files to Symantec for analysis, reinstall Norton AntiVirus.



5 Click **Finish**.



6 Click **Yes** to restart your computer.

If you have no other Symantec products on your computer, you should also uninstall LiveReg and LiveUpdate.

To uninstall LiveReg and LiveUpdate

1 Do one of the following:

- On the Windows taskbar, click **Start > Settings > Control Panel**.
- On the Windows XP taskbar, click **Start > Control Panel**.

2 In the Control Panel, double-click **Add/Remove Programs**.

3 In the list of currently installed programs, click **LiveReg**.

4 Do one of the following:

- In Windows 2000 or Windows Me, click **Change/Remove**.
- In Windows 98 or Windows NT, click **Add/Remove**.
- In Windows XP, click **Remove**.

5 Click **Yes** to confirm that you want to uninstall the product.

6 Repeat steps 1 through 5, selecting LiveUpdate in step 3, to uninstall LiveUpdate.

CHAPTER 3

Norton AntiVirus basics

Norton AntiVirus basics include general information about how to work with Norton AntiVirus, keep your computer protected, customize Norton AntiVirus, and access more information about Norton AntiVirus.

Work with Norton AntiVirus

You can perform a variety of tasks with Norton AntiVirus.

Access Norton AntiVirus tools

Norton AntiVirus tools include status reporting, scanning options, scheduling options, activity reporting, and configuration options. They can be accessed from the Norton AntiVirus main window, the Windows Explorer toolbar, and the Norton AntiVirus Windows tray icon.

Use the Norton AntiVirus main window

All Norton AntiVirus tools can be accessed from the Norton AntiVirus main window.

To start Norton AntiVirus

- Do one of the following:
  - On the Windows taskbar, click **Start > Programs > Norton AntiVirus > Norton AntiVirus 2002**.
  - On the Windows XP taskbar, click **Start > More Programs > Norton AntiVirus > Norton AntiVirus 2002**.

Use the Windows Explorer toolbar

Norton AntiVirus adds a button and menu to Windows Explorer. The button launches a scan of whatever you have selected in the Explorer pane. When you click the arrow to the right of the button, you have the following options on the Norton AntiVirus menu.

Option	Action
View Status	Launches Norton AntiVirus, displaying the Status pane with system status.
View Quarantine	Displays the Quarantine area and the files currently stored there. For more information, see "If you have files in Quarantine" on page 67.
View Activity Log	Displays the Activity Log, showing you various Norton AntiVirus activities, such as scans performed and problems found. For more information, see "Check Norton AntiVirus Activity Log" on page 38.
View Virus Encyclopedia	Connects you to the Symantec Security Response Web page, from which you can search for information on all types of viruses.
Scan for Viruses	Opens Norton AntiVirus in the Scan for Viruses pane, on which you can specify a scan to run.

When you first open Windows Explorer after installing Norton AntiVirus, you may not see the Norton AntiVirus button and menu.

To display the Norton AntiVirus button and menu

1. On the View menu, click **Toolbars**.
2. Click **Norton AntiVirus**.

Note: You may not be able to access the Norton AntiVirus Windows Explorer menu, depending on your computer's configuration. For more information, see "What's new in Norton AntiVirus" on page 11.

Use the Norton AntiVirus Windows tray icon

You can use the Norton AntiVirus Windows tray icon to open Norton AntiVirus, enable or disable Auto-Protect, and configure Norton AntiVirus. For more information, see "Temporarily disable Auto-Protect" on page 33 and "Customize Norton AntiVirus" on page 43.

To use the Norton AntiVirus Windows tray icon

1. Right-click the Norton AntiVirus Windows tray icon.
2. On the tray icon menu, select the option that you want.

Temporarily disable Auto-Protect

If you have not changed the default option settings, Auto-Protect loads when you start your computer to guard against viruses. It checks programs for viruses as they are run and monitors your computer for any activity that might indicate the presence of a virus. When a virus or *virus-like activity* (an event that could be the work of a virus) is detected, Auto-Protect alerts you.

In some cases, Auto-Protect may warn you about a virus-like activity that you know is not the work of a virus. If you will be performing such an activity and want to avoid the warning, you can temporarily disable Auto-Protect.

To temporarily disable Auto-Protect

1. Start Norton AntiVirus. For more information, see "Access Norton AntiVirus tools" on page 31.
2. At the top of the Norton AntiVirus main window, click **Options**.
3. In the Options dialog box, under System, click **Auto-Protect**.
4. In the Auto-Protect pane, uncheck **Enable Auto-Protect**.

Be sure to enable Auto-Protect when you have completed your task to ensure that your computer remains protected.

To enable Auto-Protect

1. Start Norton AntiVirus. For more information, see "Access Norton AntiVirus tools" on page 31.
2. At the top of the Norton AntiVirus main window, click **Options**.
3. In the Options dialog box, under System, click **Auto-Protect**.
4. In the Auto-Protect pane, check **Enable Auto-Protect**.

If the Norton AntiVirus icon appears in the Windows tray, you can use it to enable and disable Auto-Protect.

To enable or disable Auto-Protect using the tray icon

1. Right-click the Norton AntiVirus Windows tray icon.
2. Do one of the following:
   - If Auto-Protect is disabled, click **Enable Auto-Protect**.
   - If Auto-Protect is enabled, click **Disable Auto-Protect**.

Maintain Norton AntiVirus protection

Depending upon which operating system you are using, you may want to keep a set of Rescue Disks available and keep them up-to-date. For more information, see "If you need to use Rescue Disks" on page 70. You should also occasionally verify that Norton AntiVirus is set to provide you with optimal protection, and make sure that your virus protection is current.

About Rescue Disks

Rescue Disks record a duplicate set of system startup files and disk partition information, and store rescue items and a virus scanner across multiple floppy disks or on a network drive. Rescue Disks can be made for the DOS-based Windows 98 and Windows Me operating systems; they are not needed for Windows NT, Windows 2000, or Windows XP.

A Rescue Disk set consists of one bootable floppy disk, one Norton AntiVirus Program floppy disk, and three Virus Definition floppy disks. If you have Norton Utilities installed, you will also have two Norton Utilities floppy disks in your Rescue Disk set. With a Rescue Disk set, you can start your computer in DOS mode and use Norton AntiVirus to fix virus-related problems.

Note: Rescue Disks contain information specific to the computer on which they were made. If you are using Rescue Disks for recovery, you must use the disks made for your computer. If you are using Rescue Disks to scan for viruses, you can use disks made for a different computer. For more information, see "If you need to use Rescue Disks" on page 70.

Rescue Disks can and should be updated whenever you update your virus protection, install new software, or make changes to your hardware.

Create a Rescue Disk set

Rescue Disks can be created at any time. If you have chosen to create Rescue Disks as a post-install task in the Information Wizard, the Rescue Disk Wizard appears automatically. Otherwise, you can start the Rescue Disk Wizard from the Norton AntiVirus main window.

If you start the Rescue Disk Wizard from the Norton AntiVirus main window, temporarily disable Auto-Protect while you are creating the Rescue Disk set. If you do not restart your computer after creating Rescue Disks, remember to enable Auto-Protect again. For more information, see "Temporarily disable Auto-Protect" on page 33.

You will need several formatted 1.44 MB disks.

To create Rescue Disks

1. At the top of the Norton AntiVirus main window, click **Rescue**.

   If you chose to make Rescue Disks as a post-install task, the Rescue Disk Wizard opens automatically.
2. Select drive A to create the Rescue Disk set.
3. Click **Create**.
4. Label the disks as specified in the Basic Rescue Disk List window, then click **OK**.
5. Insert the disks as requested.

Test your Rescue Disks

At the end of the Create Rescue Disks process, you are prompted to test your disks. This requires that you restart your computer using the Rescue Disks.

To test your Rescue Disks

1. Close all open Windows programs.
2. Insert the disk labeled Basic Rescue Boot Floppy Disk into drive A, then click **Restart**.

   If the Rescue Disk screen appears on your monitor, the Rescue Disk works properly. If the Rescue Disk screen does not appear, you have several options for correcting the problem. For more information, see "My Rescue Disk does not work" on page 75.
3. Press **Escape** to exit to DOS.
4. Remove the disk from drive A, then slide open the plastic tab on the back of the disk to write-protect it.
5. Restart your computer.

Update your Rescue Disks

You can update your Rescue Disks as often as you like. Rescue Disk lets you update your basic Rescue Disks without having to recreate them.

If you are updating a floppy disk set, make sure your disks are not write-protected before you begin.

To update your Rescue Disks

1. At the top of the Norton AntiVirus main window, click **Rescue**.
2. Under Select Destination Drive, select drive A.
3. Click **Update**.
4. Insert the disk labeled Basic Rescue Boot Floppy Disk into drive A.
5. Click **OK**.
6. Insert the remaining disks in your set as requested.

Make sure to test your newly updated Rescue Disk set when prompted. For more information, see "Test your Rescue Disks" on page 36.

Check anti-virus status

If Norton AntiVirus is behaving in an unexpected way, or if you're not sure that everything is being scanned for viruses, check the status of its configuration.

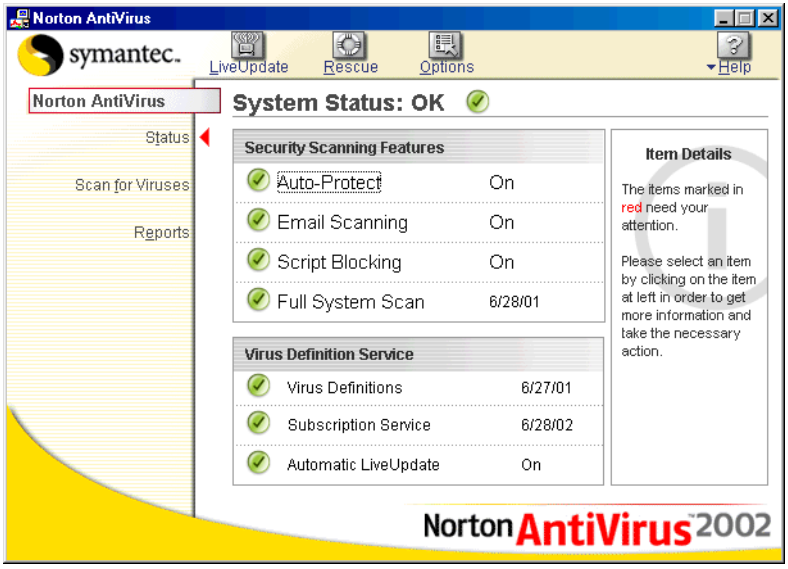
If you need to make any changes to the settings, do so using Options. For more information, see "Customize Norton AntiVirus" on page 43.

Check system status

You can check the status of most Norton AntiVirus settings in the Status pane of the Norton AntiVirus main window.

To check system status

1 Start Norton AntiVirus. For more information, see "Access Norton AntiVirus tools" on page 31.



2 Review the status displayed in the main window.

Check Office Plug-in status

Office Plug-in protects Microsoft Office documents. It scans those documents whenever you open them in an Office program. Office Plug-in is enabled in Options.

To check Office Plug-in status

1. Start Norton AntiVirus. For more information, see "Access Norton AntiVirus tools" on page 31.
2. Click **Options**.
3. On the left side of the Options window, under Other, click **Miscellaneous**.
4. Verify that Office Plug-in is enabled.

Check Norton AntiVirus Activity Log

Norton AntiVirus keeps a record of its scanning and virus detection events in the Activity Log. It is set by default to record all events; you can change this setting in Options. For more information, see "Customize Norton AntiVirus" on page 43.

You should check the Activity Log occasionally to see what tasks Norton AntiVirus has performed and the results of those tasks to make sure your Options settings are adequate.

To check the Norton AntiVirus Activity Log

1. Start Norton AntiVirus. For more information, see "Access Norton AntiVirus tools" on page 31.
2. In the Norton AntiVirus main window, click **Reports**.
3. In the Reports window, on the Activity Log line, click **View Report**.
4. Scroll through the Activity Log to see the recorded events.

   The most recent events appear at the end of the log.
5. To see only certain types of events, in the Activity Log window, click **Filter**.
6. When you are done, click **Close**.

Keep current with LiveUpdate

Symantec products depend on current information to protect your computer from newly discovered threats. Symantec makes this information available to you through LiveUpdate. Using your Internet connection, LiveUpdate downloads program updates and protection updates to your computer.

Your normal Internet access fees apply when you use LiveUpdate.

Note: If you are using Norton AntiVirus on Windows NT, Windows 2000, or Windows XP, you must have Administrator access rights to run LiveUpdate.

About program updates

Program updates are minor improvements to your installed product. These differ from product upgrades, which are newer versions of entire products. Program updates that have self-installers to replace existing software code are also called patches. Patches are usually created to extend operating system or hardware compatibility, adjust a performance issue, or fix bugs.

LiveUpdate automates the process of downloading and installing program updates. It saves you the trouble of locating and downloading files from an Internet site, then installing them, and deleting the leftover files from your disk.

About protection updates

One of the most common reasons for computer virus infections is that you have not updated your protection files regularly. Symantec provides online access to protection updates by subscription.

The virus definition service provides access to the latest virus signatures and other technology from Symantec. Norton AntiVirus, Norton SystemWorks, Norton Internet Security, and Symantec AntiVirus for Palm OS use the updates available from the virus definition service to detect the newest virus threats.

About your subscription

Your Symantec product includes a complimentary, limited time subscription to protection updates for the subscription services used by your product. When that subscription is due to expire, you are prompted to renew your subscription when you use LiveUpdate to retrieve protection updates. For more information, see "Subscription policy" on page 84.

If you do not renew your subscription, you can still use LiveUpdate to retrieve program updates. However, you cannot retrieve protection updates and will not be protected against newly discovered threats.

Obtain program and protection updates

Use LiveUpdate regularly to obtain updates. For example, to keep your virus protection current, you should use LiveUpdate once a week or whenever new viruses are discovered. Program updates are released on an as-needed basis.

Note: If you connect to the Internet through America Online (AOL), CompuServe, or Prodigy, connect to the Internet first, then run LiveUpdate.

To obtain updates using LiveUpdate

1. Open your Symantec product.
2. At the top of the window, click **LiveUpdate**.

   You might receive a warning that your subscription has expired. Follow the on-screen instructions to complete the subscription renewal.
3. Click **Next** to locate updates.
4. If updates are available, click **Next** to download and install them.
5. When the installation is complete, click **Finish**.

Run LiveUpdate automatically

You can choose to have LiveUpdate check for program and protection updates automatically, on a set schedule, by enabling automatic LiveUpdate. Once it's enabled, you can let it run according to the default schedule, or you can set when you want it to run using the Microsoft Scheduler.

Note: Automatic LiveUpdate periodically checks for an Internet connection: every five minutes until a connection is found, then every four hours. For users with ISDN routers set to automatically connect to your Internet Service Provider (ISP), this setting results in many connections being made, with connection and phone charges possibly being incurred for each connection. If this is a problem, you can set your ISDN router to not automatically connect to the ISP or disable Automatic LiveUpdate in the Norton AntiVirus options.

To enable automatic LiveUpdate

1. Start Norton AntiVirus.
2. At the top of the Norton AntiVirus main window, click **Options**.
3. In the Options dialog box, under Internet, click **LiveUpdate**.
4. In the LiveUpdate pane, check **Enable automatic LiveUpdate**.
5. Set how you want updates to be applied by selecting one of the following:
   - Apply updates without interrupting me: LiveUpdate checks for and installs protection updates without prompting you. LiveUpdate notifies you when a protection update has been downloaded. You should still run LiveUpdate occasionally to check for program updates.
   - Notify me when updates are available: LiveUpdate checks for protection updates and asks if you want to install them.
6. Click **OK**.

Automatic LiveUpdate is set by default to check for updates every four hours. To change that schedule, use the Microsoft Scheduler.

To change the automatic LiveUpdate schedule

1. On the Windows taskbar, click **Start > Programs > Accessories > System Tools > Scheduled Tasks**.
2. In the Scheduled Tasks window, double-click **Symantec NetDetect**.
3. In the scheduler dialog box, on the Schedule tab, change the default schedule as desired.

   Do not change any entries on the Task and Settings tabs.
4. Click **OK**.

You can set multiple schedules for automatic LiveUpdate.

To set multiple schedules for LiveUpdate

1. On the Windows taskbar, click **Start > Programs > Accessories > System Tools > Scheduled Tasks**.
2. In the Scheduled Tasks window, double-click **Symantec NetDetect**.
3. In the scheduler dialog box, on the Schedule tab, at the bottom of the Schedule pane, click **Show multiple schedules**.
4. At the top of the Schedule pane, click **New**.
5. Set another schedule as desired.
6. Click **OK**.

To delete the schedule for automatic LiveUpdate, disable automatic LiveUpdate.

To disable automatic LiveUpdate

1. Start Norton AntiVirus.
2. At the top of the Norton AntiVirus main window, click **Options**.
3. In the Options dialog box, under Internet, click **LiveUpdate**.
4. In the LiveUpdate pane, uncheck **Enable automatic LiveUpdate**.
5. Click **OK**.

Customize Norton AntiVirus

The default settings for Norton AntiVirus provide complete virus protection for your computer. However, you may want to adjust them to optimize system performance or disable options that do not apply.

This section does not discuss the individual options you can change, but gives a general description of what they do and how you can find them. For specific information about an option, check the online Help.

Note: If you are using Norton AntiVirus on Windows NT, Windows 2000, or Windows XP and you do not have Local Administrator access, you cannot change Norton AntiVirus options. If you are an Administrator and share your computer with others, keep in mind that the changes you make apply to everyone using the computer.

About Norton AntiVirus Options

All the settings in Options are organized into three main categories. The options contained under each category are as follows.

Category	Options
System	Auto-Protect Script Blocking Manual Scan Exclusions
Internet	Email LiveUpdate
Other	Activity Log Inoculation Miscellaneous

System options

The System options are those options that control scanning and monitoring of your computer. You use System options to determine what gets scanned, what the scan is looking for, and what happens when a virus or virus-like activity is encountered.

With higher levels of protection, there can be a slight tradeoff in computer performance. If you notice a difference in your computer's performance after you install Norton AntiVirus, you may want to set protection to a lower level or disable those options that you do not need.

Auto-Protect options

Auto-Protect options determine if Auto-Protect starts when you start your computer, what it looks for while monitoring your computer, and what it does if it finds something.

Auto-Protect also has two subcategories of options, Bloodhound and Advanced:

- Bloodhound is the scanning technology that protects against unknown viruses. Use these options to enable Bloodhound technology in Auto-Protect and set its level of sensitivity in detecting viruses. For more information, see "Bloodhound technology stops unknown viruses" on page 14.
- Advanced options determine the activities to be monitored when scanning for virus-like activities and when scanning floppy disks.

Script Blocking options

Use Script Blocking options to enable Script Blocking and set what Norton AntiVirus should do if it finds a malicious script. For more information, see "Script Blocking stops script-based viruses" on page 14.

Manual Scan options

Manual Scan options determine what gets scanned and what happens if a virus is found during a scan that you request. Manual Scan options also include a Bloodhound subcategory that lets you enable Bloodhound technology during manual scans and set its level of sensitivity in detecting viruses.

Exclusions list

The Exclusions list defines the files that should not be scanned. You can define groups of files by file extension and you can list specific files. Be careful not to exclude the types of files that are more likely to be infected by viruses, such as files with macros or executable files.

Internet options

Internet options define what happens when your computer is connected to the Internet.

Email options

Use Email options to enable email scanning and define how Norton AntiVirus should behave while scanning email. You can choose to scan incoming emails, outgoing emails, or both. Scanning incoming emails protects your computer against viruses sent by others. Scanning outgoing emails prevents you from inadvertently transmitting viruses to others.

LiveUpdate options

Use LiveUpdate options to enable Automatic LiveUpdate and define how updates should be applied. Automatic LiveUpdate checks for updated virus definitions automatically when you are connected to the Internet.

Other options

Other options include Activity Log settings, Inoculation settings, and Miscellaneous settings.

Activity Log options

The Activity Log records all Norton AntiVirus activities. You can choose to limit the activities recorded using the Activity Log options. You can also limit the size of the Activity Log. When the specified file size is reached, each new entry in the log causes the deletion of the oldest logged entry.

Inoculation options

Note: Inoculation options are available only on Windows 98, Windows 98SE, and Windows Me.

Inoculation takes a snapshot of your critical system files. If Norton AntiVirus detects changes in these system files when comparing them to the original snapshot during a scan, it warns you about the changes.

Use Inoculation options to enable inoculation and, if a system file changes, to give you the choice to update the inoculation snapshot or repair the file by restoring it to its original values.

Miscellaneous options

There are four miscellaneous options:

- Backup file in Quarantine before attempting a repair
- Enable Office Plug-in
- Alert me on startup if my virus protection is out of date
- Scan system files at startup (this option is available only for Windows 98 and Windows 98SE operating systems)

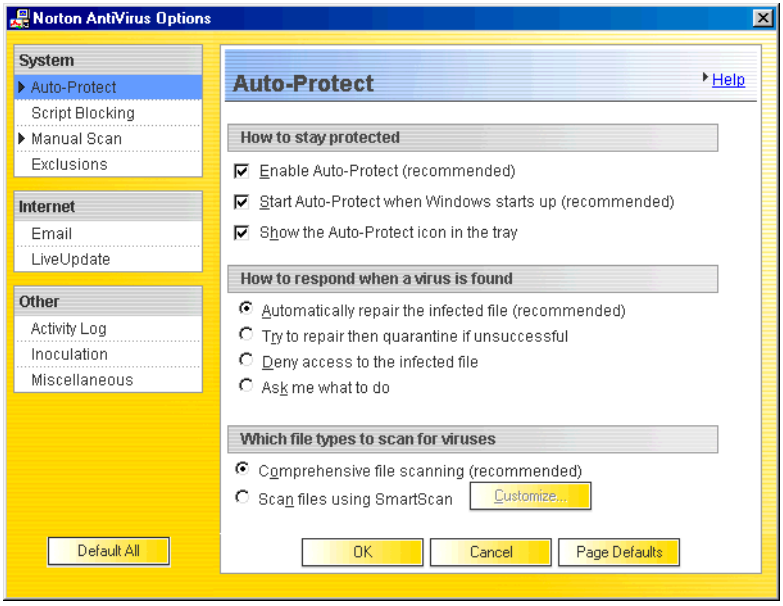
Open the Options dialog box

You change Norton AntiVirus settings in the Options dialog box.

To open the Options dialog box

1 Start Norton AntiVirus. For more information, see "Access Norton AntiVirus tools" on page 31.

2 Click **Options**.



If you need to restore default settings in Options

You can change any or all of the options listed. If you have made a number of changes that have unwanted results, you can restore all options to the default settings.

To restore default settings on a page

- On the page for which you want to restore default settings, click **Page Defaults**.

To restore default settings for all Options

- On any page in the Options dialog box, click **Default All**.

For more information

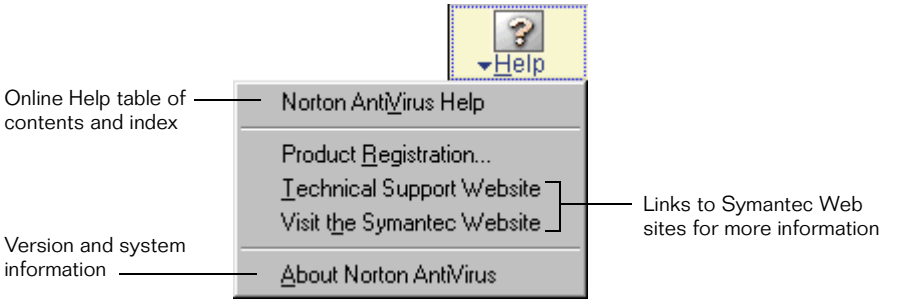
Norton AntiVirus provides online Help, this User's Guide in PDF format, and links to the Symantec Web site.

Use online Help

Help is always available from the Norton AntiVirus main window.

To access the Help menu

- At the top of the Norton AntiVirus main window, click **Help**.



In addition, Norton AntiVirus includes two kinds of more specific Help:

- Context-sensitive Help for dialog boxes
- How-to Help

Help for Norton AntiVirus dialog boxes

When you request Help while working in a Norton AntiVirus dialog box, the Help displayed is specific to that dialog box.

To get Help for a Norton AntiVirus dialog box

- In the dialog box, click **Help**.

How-to Help

How-to Help explains procedures that you are likely to perform using Norton AntiVirus. You can access these topics on the Contents and Index tabs.

To get How-to Help

1. In the Norton AntiVirus main window, click **Help**.
2. On the Help menu, click **Norton AntiVirus Help**.
3. In the Help window, select one of the following:
   - Contents: Search for Help by topic.
   - Index: Search for Help by key word.

   Contents and Index tabs are also available on many other Help windows and can always be used to search for Help.

Access the User's Guide PDF

This User's Guide is provided on the Norton AntiVirus CD in PDF format. You must have Adobe Acrobat Reader installed on your computer to read the PDF.

To install Adobe Acrobat Reader

1. Insert the Norton AntiVirus CD into the CD-ROM drive.
2. Click **Browse CD**.
3. Double-click the **Manual** folder.
4. Double-click the **Acrobat** folder.
5. Double-click **AR500ENU**.
6. Follow the on-screen instructions to select a folder for Adobe Acrobat Reader and complete the installation.

Once you have installed Adobe Acrobat Reader, you can read the PDF from the CD.

To read the User's Guide PDF from the CD

1. Insert the Norton AntiVirus CD into the CD-ROM drive.
2. Click **Browse CD**.
3. Double-click the **Manual** folder.
4. Double-click **NAV_2002**.

You can also copy the User's Guide to your hard disk and read it from there. It needs approximately 1 MB of disk space.

To read the User's Guide from your hard disk

1. Open the location into which you copied the PDF.
2. Double-click **NAV_2002**.

Norton AntiVirus on the Web

The Symantec Web site provides extensive information about Norton AntiVirus, virus protection, anti-virus technology, and other Symantec products. There are several ways to access the Symantec Web site.

To access the Symantec Web site from the Norton AntiVirus main window

1. Click **Help**.
2. Select one of the following:
   - Technical Support Web site: Takes you to the Technical Support page of the Symantec Web site, from which you can search for solutions to specific problems, update your virus protection, and read the latest information about anti-virus technology.
   - Visit the Symantec Web site: Takes you to the home page of the Symantec Web site, from which you can get product information on every Symantec product.

The Reports page of Norton AntiVirus contains a link to the Symantec online virus encyclopedia.

To access the Symantec Web site from the Reports page

1. In the Norton AntiVirus main window, click **Reports**.
2. On the Reports page, next to the Online Virus Encyclopedia heading, click **View Report**.

There is a link to the Symantec Web site on the Windows Explorer toolbar.

To access the Symantec Web site from Windows Explorer

1. Open Windows Explorer.
2. On the toolbar, on the Norton AntiVirus menu, click **View Virus Encyclopedia**.

   This option connects you to the Symantec Security Response Web page, from which you can search for information on all types of viruses.

You can always access the Symantec Web site through your Internet browser.

To access the Symantec Web site in your browser

- Type the Symantec Web site address, www.symantec.com.

CHAPTER 4

Protecting disks, files, and data from viruses

Keeping your computer protected requires regular monitoring by Auto-Protect, scanning of your email, and frequent system scans. All of these tasks can be set to occur automatically.

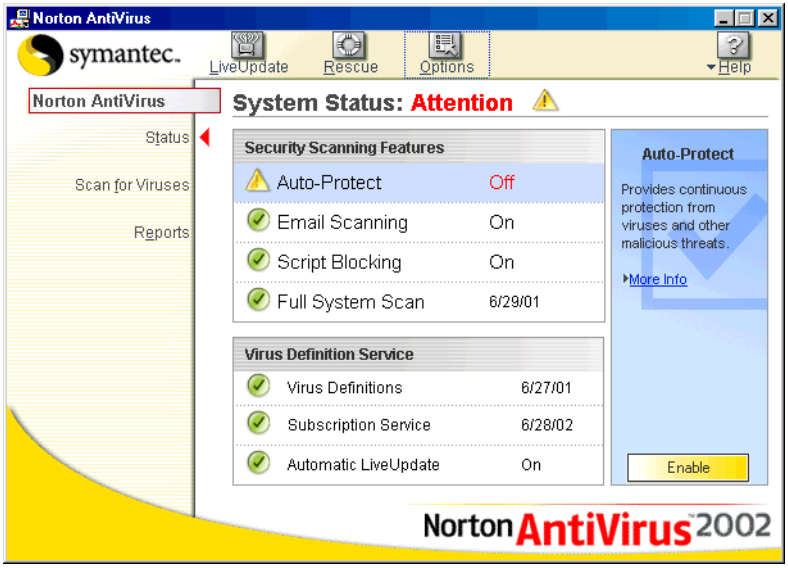
Ensure that Auto-Protect is enabled

Norton AntiVirus is configured to provide you with complete protection against viruses. It is unlikely that you need to change any settings. However, you can ensure that Auto-Protect is working by following these steps.

To ensure that Auto-Protect is enabled

1. Start Norton AntiVirus.
2. In the Status pane of the Norton AntiVirus main window, ensure that Auto-Protect is set to On.

3 If Auto-Protect is not enabled, in the Status pane, select the Auto-Protect status line.



4 In the lower right-hand corner of the window, click **Enable**.

Scan disks, folders, and files

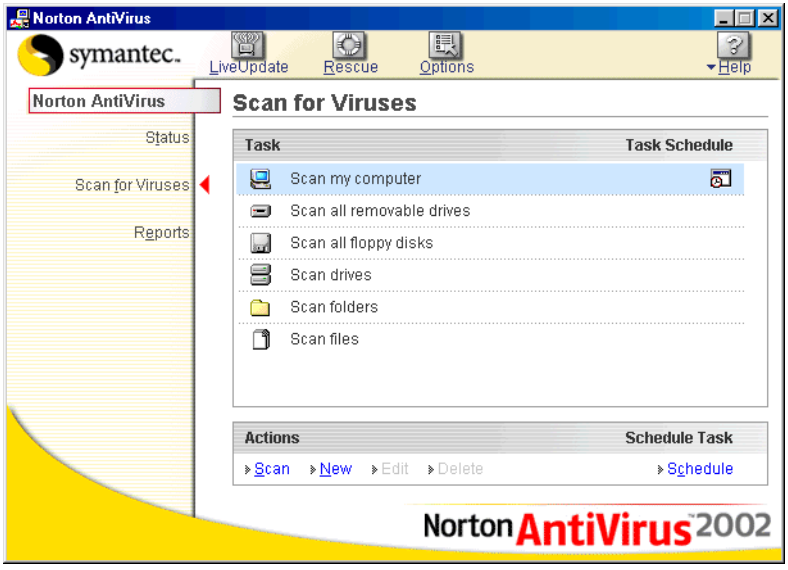
You can request scans of your entire computer, or of individual elements such as floppy disks, drives, folders, or files.

Request a full system scan

A full system scan scans all boot records and files on your computer.

To request a full system scan

1. Start Norton AntiVirus.
2. In the Norton AntiVirus main window, click **Scan for Viruses**.



3. In the Scan for Viruses pane, click **Scan my computer**.
4. Under Actions, click **Scan**.

   When the scan is complete, a scan summary appears.
5. When you are done reviewing the summary, click **Finished**.

Scan individual elements

You can choose to scan all removable drives, a floppy disk, any of your computer's drives, or any folders or files on your computer.

To scan individual elements

1. Start Norton AntiVirus.
2. In the Norton AntiVirus main window, click **Scan for Viruses**.
3. In the Scan for Viruses pane, click the scan you want to run.
4. Under Actions, click **Scan**.

   If you choose to scan all removable drives or a floppy disk, the scan starts automatically.

   If you choose to scan drives, folders, or files, a dialog box appears in which you choose which drives, folders, or files to scan. Click **Scan** after making your selection.

   When the scan is complete, a scan summary appears.
5. When you are done reviewing the summary, click **Finished**.

About custom scans

You can create a custom scan if you regularly scan a particular segment of your computer and don't want to have to specify the segment to be scanned every time. You can delete the scan when it is no longer necessary. For example, if you are working on a project for which you need to frequently swap files with others, you might want to create a folder into which you copy and scan those files before using them. When the project is done, you can delete the custom scan for that folder.

You can also schedule the custom scan to run automatically. For more information, see "Schedule a custom scan" on page 60.

Create a custom scan

You can create a custom scan that includes as much or as little of your computer as you like.

To create a custom scan

1. Start Norton AntiVirus.
2. In the Norton AntiVirus main window, click **Scan for Viruses**.
3. In the Scan for Viruses pane, under Actions, click **New**.
4. In the opening window of the Norton AntiVirus Scan Wizard, click **Next**.
5. Select what you want to scan by doing one or both of the following:
   - To select individual files to be scanned, click **Add files**.
   - To select folders and drives to be scanned, click **Add folders**.

   You can use both options to select the combination of items that you want.
6. Select the items that you want to scan in the resulting dialog box.

   If you select a folder, all files in that folder are included. If you select a drive, all folders and files on that drive are included.
7. Add the selected items to the list of items to scan by doing one of the following:
   - In the Scan Files dialog box, click **Open**.
   - In the Scan Folders dialog box, click **Add**.
8. To remove an item from the list, select it, then click **Remove**.
9. When you are done creating the list of items to be scanned, click **Next**.
10. Type a name for the scan by which you can identify it in the list of scans.
11. Click **Finish**.

Run a custom scan

When you run a custom scan, you do not have to redefine what you want to scan.

To run a custom scan

1. Start Norton AntiVirus.
2. In the Norton AntiVirus main window, click **Scan for Viruses**.
3. In the Scan for Viruses pane, click the custom scan.
4. Under Actions, click **Scan**.

   When the scan is complete, a scan summary appears.
5. When you are done reviewing the summary, click **Finished**.

Delete a custom scan

Custom scans can be deleted if they are no longer needed.

To delete a custom scan

1. Start Norton AntiVirus.
2. In the Norton AntiVirus main window, click **Scan for Viruses**.
3. Select the scan that you want to delete by clicking the scan name.

   If you click the button next to the scan name, the scan runs.
4. Under Actions, click **Delete**.
5. Click **Yes** to verify that you want the scan deleted.

Scan email messages

If email protection is enabled, your email messages are scanned automatically. Norton AntiVirus supports all email programs that use either POP3 or SMTP communications protocol. To prevent connection timeouts while receiving large attachments, enable timeout protection.

Ensure that email protection is enabled

You can choose to scan incoming or outgoing email, or both. If your email program uses one of the supported communications protocols, both options are selected by default. You can check or change these settings using Options.

To ensure that email protection is enabled

1. Start Norton AntiVirus.
2. In the Norton AntiVirus main window, click **Options**.
3. In the Options window, under Internet, click **Email**.
4. For complete email protection, ensure that both Scan incoming Email and Scan outgoing Email are checked.

   To disable one of the options, uncheck it.
5. Click **OK**.

Enable timeout protection

Norton AntiVirus scans email by monitoring the communications port used for email and intercepting email transmissions. Only after incoming email has been scanned is it passed along to the email program. If you are downloading email with a large attachment, your email program may not receive a transmission for a few minutes and may timeout as a result. If you enable timeout protection, Norton AntiVirus regularly confirms the connection with your email program and prevents a timeout.

Note: Timeout protection places hidden text at the top of your email messages. Your email program should remove this text. If you see "NAV Timeout Protection" in your email messages, you can ignore it.

To enable timeout protection

1. Start Norton AntiVirus.
2. In the Norton AntiVirus main window, click **Options**.
3. In the Options window, under Internet, click **Email**.
4. Ensure that Protect against timeouts when scanning Email is checked.
5. Click **OK**.

If problems are found during a scan

At the end of a scan, a summary report appears to tell you what Norton AntiVirus found during the scan. If a virus was found and you have requested that Norton AntiVirus repair the file automatically, it is listed as repaired.

If the file cannot be repaired, it can be quarantined or deleted. For more information, see "If a virus is found during a scan" on page 64.

Schedule automatic virus scans

When you install Norton AntiVirus and complete the Information Wizard, you can choose to schedule a weekly full system scan as part of post-install tasks. If you make that choice, the scan is scheduled automatically.

Note: You cannot schedule the predefined scans in the scan list, but you can schedule any custom scans that you have created.

Schedule a custom scan

You have complete flexibility in scheduling custom scans. When you select how frequently you want a scan to run (such as daily, weekly, or monthly), you are presented with additional fields with which you can refine your request. For example, you can request a daily scan, then schedule it to occur every two days or every three days instead.

To schedule a scan

1. Start Norton AntiVirus.
2. In the Norton AntiVirus main window, click **Scan for Viruses**.
3. Select the scan that you want to schedule by clicking the scan name.

   If you click the button next to the scan name, the scan runs.
4. Click **Schedule**.
5. In the scheduling dialog box, if Show multiple schedules is checked, click **New** to enable the scheduling fields.

   If it is not checked, the fields will already be enabled.

6 Set the frequency and time at which you want the scan to run.

Most of the frequency options include additional options that let you further refine the schedule. Set the additional options as necessary.

7 When you are done, click **OK**.

You can also create multiple schedules for a scan. For example, you could run the same scan at the beginning of your work day and at the end.

To create multiple schedules for a single scan

1 Start Norton AntiVirus.

2 In the Norton AntiVirus main window, click **Scan for Viruses**.

3 Select the scan that you want to schedule by clicking the scan name.

If you click the button next to the scan name, the scan runs.

4 Click **Schedule**.

5 In the scheduling dialog box, check **Show multiple schedules**.

6 To set an additional schedule, click **New**.

7 Set the frequency and time at which you want the scan to run.

Most of the frequency options include additional options that let you further refine the schedule. Set the additional options as necessary.

8 When you are done, click **OK**.

Edit scheduled scans

You can change the schedule of any scheduled scan, including the weekly full system scan.

To edit a scheduled scan

1 Start Norton AntiVirus.

2 In the Norton AntiVirus main window, click **Scan for Viruses**.

3 Select the scan that you want to schedule by clicking the scan name.

If you click the button next to the scan name, the scan runs.

4 Click **Schedule**.

5 Change the schedule as desired.

6 Click **OK**.

Delete a scan schedule

You can delete any scan schedule. Deleting the schedule does not delete the scan.

To delete a scan schedule

1. Start Norton AntiVirus.
2. In the Norton AntiVirus main window, click **Scan for Viruses**.
3. Select the scan you want to schedule by clicking the scan name.

   If you click the button next to the scan name, the scan runs.
4. Click **Schedule**.
5. In the scheduling dialog box, check **Show multiple schedules** to display the Delete button.
6. Select the schedule that you want to delete (if more than one), then click **Delete**.
7. Click **OK**.

C H A P T E R 5

What to do if a virus is found

If Norton AntiVirus finds a virus on your computer, there are three possible resolutions to the problem:

- Repair the file. This action removes the virus from the file.
- Quarantine the file. This action makes the file inaccessible by any programs other than Norton AntiVirus. You cannot accidentally open the file and spread the virus, but you can still evaluate it for possible submission to Symantec. For more information, see "If you have files in Quarantine" on page 67.
- Delete the file. This action removes the virus from your computer by deleting the file that contains the virus. It should be used only if the file cannot be repaired or quarantined.

Viruses can be found when you run a scan or by Auto-Protect when you perform an action with an infected file. The way that you request one of these resolutions differs depending on whether a scan or Auto-Protect found the virus.

If a virus is found during a scan

If a scan you request finds a virus, you either receive a summary of the repair results, or you have to use the Repair Wizard to resolve the problem.

Review the repair details

If you have set your manual scan options so that Norton AntiVirus repairs files automatically, and all infected files could be repaired, the scan summary lists the number of files infected and repaired. This information is presented for status purposes only; you don't need to take further action to protect your computer. If you want to know more, you can check the repair details to see which files were infected and with what.

To review the repair details

1. In the Summary pane of the scanner window, click **More Details**.
2. When you are done reviewing the results, click **Finished**.

Use the Repair Wizard

If there are files that could not be repaired, or if you have set your manual scan options so that Norton AntiVirus asks you what to do when a virus is found, the Repair Wizard opens.

If Norton AntiVirus did not attempt a repair, the Repair Wizard opens in the Repair pane. Otherwise, it opens in the Quarantine pane.

To use the Repair Wizard

1. If the Repair Wizard opens in the Repair pane, uncheck any files that you don't want Norton AntiVirus to repair.

   All files are checked by default. This is the recommended action.
2. Click **Repair**.
3. If any files cannot be repaired, the Quarantine pane opens.

   All files are checked to be added to quarantine by default. This is the recommended action.

   In the Quarantine pane, uncheck any files that you do not want to quarantine, then click **Quarantine**.

4 If any files could not be quarantined, the Delete pane opens.

If you do not delete the infected files, the virus remains on your computer and can cause damage or be transmitted to others.

Uncheck any files that you do not want to be deleted, then click **Delete**.

5 Once all files have either been repaired, quarantined, or deleted, the Summary pane of the scanner window opens. When you are done reviewing the summary, click **Finished**.

If a virus is found by Auto-Protect

Auto-Protect scans files for viruses when you perform some action with them, such as moving them, copying them, or opening them. If it detects a virus or virus-like activity, in most cases you receive an alert telling you that a virus was found and repaired. How you proceed from there depends on the operating system you are using.

If you are using Windows 98/98SE/Me

If a virus is found and repaired by Auto-Protect in Windows 98, Windows 98SE, or Windows Me, you receive an alert telling you what file was repaired.

To close the alert

- Click **Finish**.

If you have set your options so that Auto-Protect asks you what to do when it finds a virus, the alert asks you to choose an action. The recommended action is always preselected. If you are not sure what action you should select, use this table to decide.

Action	Result
Repair the infected file	Eliminates the virus and repairs the infected item. When a virus is found, Repair is always the best choice.
Quarantine the infected file	Isolates the virus-infected file, but does not remove the virus. Select Quarantine if you suspect that the infection is caused by an unknown virus and you want to submit the virus to Symantec for analysis.

Action	Result
Delete the infected file	Erases both the virus and the infected file. Select Delete if Repair is not successful. Replace the deleted file from the original program file or backup copy. If the virus is detected again, your original copy is infected.
Do not open the file, but leave the problem alone	Stops the current operation to prevent you from using an infected file. This action does not solve the problem. You will receive an alert the next time you perform the same activity.
Ignore the problem and do not scan this file in the future	Adds the file suspected of containing a virus to the Exclusions list. When you add a file to the Exclusions list, the file will be excluded from any future virus scans, unless you remove it from the list. Select this option only if you know that the file does not contain a virus.
Ignore the problem and continue with the infected file	Continues the current operation. Select this action only if you are sure that a virus is not at work. You will receive an alert again. If you are not sure what to do, select Do not open the file, but leave the problem alone.

If the file could not be repaired, you receive an alert telling you that the repair was not made and recommending that you quarantine the file. You have the same options as those listed in the table, with the exception of Repair the infected file.

If you are using Windows NT/2000/XP

If a virus is found and repaired by Auto-Protect in Windows NT, Windows 2000, or Windows XP, you receive an alert telling you what file was repaired and what virus was infecting the file. If you have an active Internet connection, clicking the virus name opens the Symantec Web page that describes the virus.

To close the alert

- Click **OK**.

If the file could not be repaired, you receive two alerts, one telling you that Auto-Protect was unable to repair the file and the other telling you that access to the file was denied.

You can set your Auto-Protect options to try to quarantine any infected files it cannot repair. If you do so, you are informed if any files are quarantined. For more information, see "If you have files in Quarantine" on page 67.

To resolve problems with unrepaired files

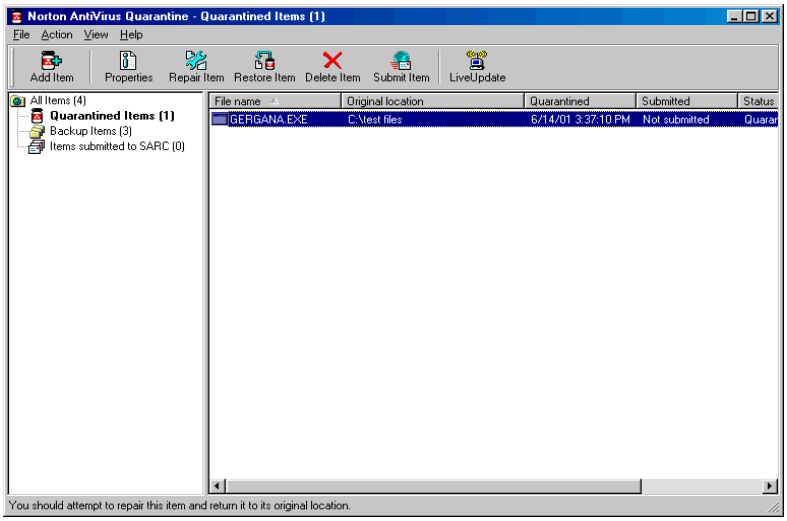
1. Run a manual scan on your computer to ensure that no other files are infected. For more information, see "Request a full system scan" on page 55.
2. Follow the recommended actions in the Repair Wizard to protect your computer from the infected files. For more information, see "If a virus is found during a scan" on page 64.

If you have files in Quarantine

Once a file has been placed in Quarantine, you have several options. All actions on files in Quarantine must be performed using the Quarantine window.

To open the Quarantine window

1. Start Norton AntiVirus.
2. In the Norton AntiVirus main window, click **Reports**.
3. In the Reports pane, on the Quarantined items line, click **View Report**.



The buttons across the top of the Quarantine window represent all of the actions you can perform on the files in Quarantine. The following actions are available.

Action	Result
Add Item	Adds files to Quarantine. Use this action to quarantine a file that you suspect is infected. This action has no effect on the files already in Quarantine.
Properties	Provides detailed information about the selected file and what is infecting it.
Repair Item	Attempts to repair the selected file. Use this action if you have received new virus definitions since the file was added to Quarantine.
Restore Item	Returns the selected file to its original location without repairing it.
Delete Item	Deletes the selected file from your computer.
Submit Item	Sends the selected file to Symantec. Use this option if you suspect that a file is infected even if Norton AntiVirus did not detect a virus, or if you suspect that the virus is one that was newly released.
LiveUpdate	Runs LiveUpdate to check for new protection and program updates. Use this if you haven't updated your virus protection for a while and want to try to repair the files in Quarantine.

To perform an action on a file in Quarantine

1. Select the file on which you want to perform the action.
2. Click the button for the action that you want to perform.
3. When you are finished, on the File menu, click **Exit**.

If Norton AntiVirus cannot repair a file

One of the most common reasons Norton AntiVirus cannot repair a file is that you do not have the most up-to-date virus protection. Update your virus protection with LiveUpdate and scan again. For more information, see "Keep current with LiveUpdate" on page 39.

If that does not work, read the information on your screen to identify the type of item that cannot be repaired, and then match it to one of the types below:

- Infected files are those with file name extensions such as .exe, .doc, .dot, or .xls. Files with any name can be infected. Use the Repair Wizard to solve the problem. For more information, see "Use the Repair Wizard" on page 64.
- Hard disk master boot record, boot record, or system files (such as IO.SYS or MSDOS.SYS) and floppy disk boot record and system files are replaced using the Rescue Disks or your operating system disks. For more information, see "If you need to use Rescue Disks" on page 70.

If your computer does not start properly

If you have a virus on your computer and need to start the computer from an uninfected disk to remove the virus, or if you need to restore a boot record, use your Rescue Disks. If you do not have Rescue Disks, you can use your Emergency Disks to start the computer and remove the virus. If you need to restore boot records and do not have Rescue Disks, or if you need to restore system files, you must reinstall Windows. For more information, see "About Rescue Disks" on page 34 and "Create Emergency Disks" on page 19.

If you need to use Rescue Disks

Sometimes a virus infection prevents your computer from starting normally. Some viruses can only be removed if the computer is started from a clean disk, not the infected hard disk. Often, a Norton AntiVirus alert tells you when to use your Rescue Disks.

You first need to determine whether your Rescue Disks are current. This means that you have created or updated your Rescue Disks since you did any of the following:

- Added, modified, or removed internal hardware
- Added, modified, or removed hard disk partitions
- Upgraded your operating system

If your Rescue Disks are not current, you can still use them to remove viruses from your computer. When the Rescue Disk screen starts from the Rescue Boot disk, use only the Norton AntiVirus task.

To use your Rescue Disks

1. Insert the Basic Rescue Boot floppy disk into the floppy disk drive and restart your computer.

   The Rescue program runs in DOS.

2. Use the arrow keys to highlight the program that you want to run.

   A description of the highlighted program appears in the right panel of the Rescue program. Your choices are:

   - Norton AntiVirus. Scans your computer for viruses and repairs any infected files.
   - Rescue Recovery. Checks and restores boot and partition information.

3. Press **Enter** to run the highlighted program.
4. Follow the on-screen instructions for inserting and removing the Rescue Disks.
5. When the Rescue program is done, remove the Rescue Disk in the floppy disk drive and restart your computer.

If you need to use Emergency Disks

Use the following procedures if you need to use your Emergency Disks. For more information, see "Create Emergency Disks" on page 19.

To use Emergency Disks

1. Insert Emergency Disk 1 into the floppy disk drive and restart your computer.

   The Emergency program runs in DOS.
2. Ensure that Antivirus is selected and press **Enter** to begin the Norton AntiVirus Emergency program.
3. Follow the on-screen instructions for inserting and removing the Emergency Disks.

   The Emergency program automatically scans your computer and removes viruses.
4. When the Emergency program is done, remove the Emergency Disk in the floppy disk drive and restart your computer.

If you are using the CD as an Emergency Disk

If you are using the Norton AntiVirus CD as an Emergency Disk, use this procedure whenever you are instructed to insert Emergency Disk 1. You can ignore all instructions to change disks, as all necessary information is on the CD.

Note: You may need to change your computer's BIOS Setup options to start from the CD-ROM drive. For more information, see "I cannot start from drive A" on page 76.

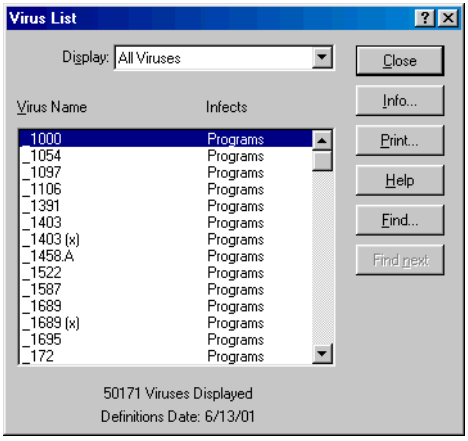
To use the CD as an Emergency Disk

1. Insert the Norton AntiVirus CD into the CD-ROM drive.
2. Restart your computer.

   The Emergency program scans your computer and removes viruses.

Look up virus names and definitions

You can look up a virus name from within Norton AntiVirus. The Virus List dialog box lists the viruses in the current virus definition service files.



To make sure that you have the latest virus definitions, run LiveUpdate. For more information, see "Keep current with LiveUpdate" on page 39.

To look up virus names

1. Start Norton AntiVirus.
2. In the Norton AntiVirus main window, click **Reports**.
3. In the Reports pane, on the Virus List line, click **View Report**.

You can print the list.

To print the list

- In the Virus List dialog box, click **Print**.

You can also use the list to get more information about a specific virus.

To get more information about a specific virus

1. In the Virus List dialog box, select the virus about which you want more information.
2. Click **Info**.
3. When you are done viewing the virus information, in the Virus Information window, click **Close**.
4. When you are done viewing the list, in the Virus List dialog box, click **Close**.

Look up viruses on the Symantec Web site

Because of the large number of viruses, the Virus List file does not include descriptions of each virus. The Symantec Web site contains a complete list of all known viruses and related malicious code, along with descriptions.

To look up viruses

1. In the Norton AntiVirus main window, click **Reports**.
2. In the Reports pane, on the Online Virus Encyclopedia line, click **View Report**.

   The Symantec Web site opens in your Internet browser.
3. Use the links on the Web page to access the virus information for which you are looking.

CHAPTER 6

Troubleshooting

The information in this chapter will help you solve the most frequent problems that you may experience. If you can't find the solution to your problem here, there is a wealth of information on the Symantec Web site. You can find a troubleshooter, updates, patches, online tutorials, knowledge base articles, and virus removal tools. Point your browser to www.symantec.com/techsupp/.

My Rescue Disk does not work

Due to the number of product-specific technologies used by manufacturers to configure and initialize hard drives, the Rescue program cannot always create a bootable disk automatically. If your Rescue Boot Disk does not work properly, do one of the following:

- If you have a special startup disk for your computer, add it to your Rescue Disk set. In an emergency, start from that disk. Remove the disk and insert your Rescue Boot Disk. At the DOS prompt, type `A:RSHELL`, press Enter, then follow the on-screen instructions.
- Use the Disk Manager or similarly named program that came with your computer to make your Rescue Boot Disk bootable. Make sure to test your modified Rescue Boot Disk.

Sometimes, your Rescue Boot Disk does not work properly because you have more than one operating system installed, such as Windows NT and Windows 98.

To modify your Rescue Boot Disk

1. Start up from your hard drive.
2. Insert your Rescue Boot Disk into drive A.
3. At the DOS prompt, type **SYS A:**
4. Press **Enter**.

   This transfers the operating system to the Rescue Boot Disk. Be sure to retest your Rescue Disks.

The alert tells me to use my Rescue Disks, but I did not create them

With your Norton AntiVirus CD you can create Emergency Disks. Although they are not as powerful as the Rescue Disks you create, you can use the Emergency Disks to recover from most common emergencies. For more information, see "To create Emergency Disks" on page 19.

You can use the CD that contains Norton AntiVirus as an Emergency Disk if your computer can start from the CD-ROM drive. For more information, see "If you are using the CD as an Emergency Disk" on page 71.

Once you have created the Emergency Disks, use them to solve the problem.

I cannot start from drive A

If your computer does not check drive A first on startup, use your computer's Setup program to change settings.

Be careful when making changes using your computer's Setup program. If you have never used it before, you may want to refer to your computer manufacturer's documentation.

To change your computer's settings

1. Restart your computer.

   A message appears telling you the key or keys to press to run SETUP, such as Press <DEL> if you want to run SETUP.
2. Press the key or keys to launch the Setup program.
3. Set the Boot Sequence to boot drive A first and drive C second.

   Setup programs vary from one manufacturer to the next. If you cannot find the Boot Sequence option, use the Setup program's Help system, refer to the documentation that came with your system, or contact your system's manufacturer.
4. Save the changes, then exit the Setup program.

You may need to use a special boot disk rather than the Rescue Boot Disk. In this case, use the boot disk or startup disk that came with your computer.

If your computer is set up with more than one operating system, such as Windows 2000 and Windows 98, you may need to modify the Rescue Boot Disk. For more information, see "My Rescue Disk does not work" on page 75.

Norton AntiVirus Auto-Protect does not load when I start my computer

If the Norton AntiVirus Auto-Protect icon does not appear in the lower-right corner of the Windows taskbar, Auto-Protect is not loaded. There are three likely reasons this is happening.

You may have started Windows in safe mode. Windows restarts in safe mode if the previous shutdown did not complete successfully. For example, you may have turned off the power without choosing Shut Down on the Windows Start menu.

To restart Windows

1. On the Windows taskbar, click **Start > Shut Down**.
2. In the Shut Down Windows dialog box, click **Restart**.
3. Click **OK**.

Norton AntiVirus may not be configured to start Auto-Protect automatically.

To set Auto-Protect to start automatically

1. In the Norton AntiVirus main window, click **Options**.
2. In the Options dialog box, under System, click **Auto-Protect**.
3. Ensure that Start Auto-Protect when Windows starts up is checked.

Norton AntiVirus may not be configured to show the Auto-Protect icon in the tray.

To show the Auto-Protect icon in the tray

1. In the Norton AntiVirus main window, click **Options**.
2. In the Options dialog box, under System, click **Auto-Protect**.
3. Ensure that Show the Auto-Protect icon in the tray is checked.

I have scanned and removed a virus, but it keeps infecting my files

There are four possible reasons a virus could be reappearing.

The virus might be in a program file with an unusual extension for which Norton AntiVirus is not configured to look.

To reset Norton AntiVirus scanning options

1. In the Norton AntiVirus main window, click **Options**.
2. In the Options dialog box, under System, click **Manual Scan**.
3. Under Which file types to scan for viruses, click **Comprehensive file scanning**.
4. Click **Manual Scan > Bloodhound**.
5. Ensure that Enable Bloodhound heuristics is checked, and click **Highest level of protection**.
6. Click **OK**.
7. Scan all of the disks that you use and repair all infected files.

The source of the infection could also be a floppy disk. Scan all of the floppy disks that you use to ensure that they are free of viruses.

Another reason could be that the virus is remaining in memory after you remove it from the boot record. It then reinfects your boot record. Use your Rescue Disks to remove the virus. For more information, see "If you need to use Rescue Disks" on page 70.

If the problem is a Trojan horse or worm that was transmitted over a shared network drive, you must disconnect from the network or password protect the drive to let Norton AntiVirus delete the problem.

Norton AntiVirus cannot repair my infected files

The most common reason that Norton AntiVirus cannot repair your infected files is that you do not have the most current virus protection on your computer. Update your virus protection regularly to protect your computer from the latest viruses. For more information, see "Keep current with LiveUpdate" on page 39.

If after using LiveUpdate the virus still cannot be repaired, the file may be corrupted, or contain a new virus. There are two additional options:

- Quarantine the file and submit it to Symantec. For more information, see "If you have files in Quarantine" on page 67.
- If a non-infected copy of the file exists, delete the infected file and replace it with the non-infected file.

I get an error when testing basic Rescue Disks

If you get the message Non-system disk, replace disk and press any key when testing your Rescue Disks, the Rescue program may not have prepared the floppy boot files correctly.

To repair the Rescue Boot Disk without having to reformat the disk and create a new Rescue Disk set

1. Remove the Rescue Boot Disk and restart your computer.
2. Insert the Rescue Boot Disk into the floppy disk drive.
3. On the Windows taskbar, click **Start > Run**.
4. In the Run dialog box, type **SYS A:**
5. Click **OK**.

I can't receive email

There are three possible solutions to this problem.

Temporarily disable email protection. This might allow the problem email to be download so that you can once again enable email protection. You are protected by Auto-Protect and Script Blocking while email protection is disabled.

To temporarily disable incoming email protection

1. In the Norton AntiVirus main window, click **Options**.
2. In the Options dialog box, under Internet, click **Email**.
3. Uncheck **Scan incoming Email**.
4. Click **OK**.
5. Download your email.
6. Reenable incoming email protection.

Your email client may have timed out. Make sure timeout protection is enabled. For more information, see "Enable timeout protection" on page 59.

If you continue to experience problems downloading email, disable email protection.

To disable email protection

1. In the Norton AntiVirus main window, click **Options**.
2. In the Options dialog box, under Internet, click **Email**.
3. Uncheck **Scan incoming Email**.
4. Uncheck **Scan outgoing Email**.
5. Click **OK**.

Service and support solutions

Service and support information is available from the Help system of your Symantec product. Click the Service and Support topic in the Help index.

Technical support

Symantec offers several technical support options:

- Online Service and Support

  Connect to the Symantec Service & Support Web site at http://service.symantec.com, select your user type, and then select your product and version. This gives you access to current hot topics, knowledge bases, file download pages, multimedia tutorials, contact options, and more.

- PriorityCare telephone support

  PriorityCare fee-based telephone support services are available to all registered customers. For complete information, please call our automated fax retrieval service at (800) 554-4403 and request document 933000.

  You can also access the PriorityCare number for your product through the Service & Support Web site. You'll be led through the online options first, and then to the telephone contact options available for your product and version.

- Automated fax retrieval

  Use your fax machine to receive general product information, fact sheets, and product upgrade order forms by calling (800) 554-4403. For technical application notes, call (541) 984-2490.

Support for old and discontinued versions

When a new version of this software is released, registered users will receive upgrade information in the mail. Telephone support will be provided for the old version for up to twelve months after the release of the new version. Technical information may still be available through the Service & Support Web site (http://service.symantec.com).

When Symantec announces that a product will no longer be marketed or sold, telephone support will be discontinued 60 days later. Support will be available for discontinued products from the Service & Support Web site only.

Customer service

Access customer service options through the Service & Support Web site at http://service.symantec.com. From this site, you can receive assistance with non-technical questions, and for information on how to do the following:

- Subscribe to the Symantec Support Solution of your choice.
- Obtain product literature or trialware.
- Locate resellers and consultants in your area.
- Replace missing or defective CD-ROMS, disks, manuals, and so on.
- Update your product registration with address or name changes.
- Get order, return, or rebate status information.
- Access customer service FAQs.
- Post a question to a Customer Service representative.

For upgrade orders, visit the online upgrade center at:
http://www.symantecstore.com

Worldwide service and support

Technical support and customer service solutions vary by country. For information on Symantec and International Partner locations outside of the United States, please contact one of the service and support offices listed below, or connect to http://service.symantec.com and select your region under the Global Service and Support.

Service and support offices

North America

Symantec Corporation
175 W. Broadway
Eugene, OR 97401
U.S.A.

http://www.symantec.com/
Fax: (541) 984-8020

Automated Fax Retrieval

(800) 554-4403
(541) 984-2490

Argentina and Uruguay

Symantec Region Sur
Cerrito 1054 - Piso 9
1010 Buenos Aires
Argentina

http://www.service.symantec.com/mx
+54 (11) 5382-3802

Asia/Pacific Rim

Symantec Australia
Level 2, 1 Julius Avenue
North Ryde, NSW 2113
Sydney
Australia

http://www.symantec.com/region/reg_ap/
+61 (2) 8879-1000
Fax: +61 (2) 8879-1001

Brazil

Symantec Brasil
Market Place Tower
Av. Dr. Chucri Zaidan, 920
12° andar
São Paulo - SP
CEP: 04583-904
Brasil, SA

http://www.service.symantec.com/br
+55 (11) 5189-6300
Fax: +55 (11) 5189-6210

Europe, Middle East, and Africa

Symantec Customer Service Center
P.O. Box 5689
Dublin 15
Ireland

http://www.symantec.com/region/reg_eu/
+353 (1) 811 8032

Mexico

Symantec Mexico
Blvd Adolfo Ruiz Cortines,
No. 3642 Piso 14
Col. Jardines del Pedregal
Ciudad de México, D.F.
C.P. 01900
México

http://www.service.symantec.com/mx
+52 (5) 661-6120

Other Latin America

Symantec Corporation
9100 South Dadeland Blvd.
Suite 1810
Miami, FL 33156
U.S.A.

http://www.service.symantec.com/mx

Subscription policy

If your Symantec product includes virus, firewall, or web content protection, you might be entitled to receive protection updates via LiveUpdate. The length of the subscription could vary by Symantec product.

When you near the end of your subscription, you will be prompted to subscribe when you start LiveUpdate. Simply follow the instructions on the screen. After your initial subscription ends, you must renew your subscription before you can update your virus, firewall, or web content protection. Without these updates, your vulnerability to attack increases. Renewal subscriptions are available for a nominal charge.

Every effort has been made to ensure the accuracy of this information. However, the information contained herein is subject to change without notice. Symantec Corporation reserves the right for such change without prior notice.

July 13, 2001

Norton AntiVirus™

CD Replacement Form

CD REPLACEMENT: After your 60-Day Limited Warranty, if your CD becomes unusable, fill out and return 1) this form, 2) your damaged CD, and 3) your payment (see pricing below, add sales tax if applicable), to the address below to receive replacement CD. *DURING THE 60-DAY LIMITED WARRANTY PERIOD, THIS SERVICE IS FREE.* You must be a registered customer in order to receive CD replacements.

FOR CD REPLACEMENT

Please send me: ___ CD Replacement

Name _____

Company Name _____

Street Address (No P.O. Boxes, Please)_____

City _____ State _____ Zip/Postal Code _____

Country* _____Daytime Phone _____

Software Purchase Date _____

*This offer limited to U.S., Canada, and Mexico. Outside North America, contact your local Symantec office or distributer.

Briefly describe the problem:_____

_____

CD Replacement Price	$ 10.00
Sales Tax (See Table)	_____
Shipping & Handling	$ 9.95
TOTAL DUE	_____

SALES TAX TABLE: AZ (5%), CA (7.25%), CO (3%), CT (6%), DC (5.75%), FL (6%), GA (4%), IA (5%), IL (6.25%), IN (5%), KS (4.9%), LA (4%), MA (5%), MD (5%), ME (6%), MI (6%), MN (6.5%), MO (4.225%), NC (6%), NJ (6%), NY (4%), OH (5%), OK (4.5%), PA (6%), SC (5%), TN (6%), TX (6.25%), VA (4.5%), WA (6.5%), WI (5%). Please add local sales tax (as well as state sales tax) in AZ, CA, FL, GA, MO, NY, OH, OK, SC, TN, TX, WA, WI.

FORM OF PAYMENT ** (CHECK ONE):

___ Check (Payable to Symantec) Amount Enclosed $ _____ __ Visa __ Mastercard __ American Express

Credit Card Number _____Expires _____

Name on Card (please print) _____ Signature _____

****U.S. Dollars. Payment must be made in U.S. dollars drawn on a U.S. bank.**

MAIL YOUR CD REPLACEMENT ORDER TO:

Symantec Corporation
Attention: Order Processing
175 West Broadway
Eugene, OR 97401-3003 (800) 441-7234

Please allow 2-3 weeks for delivery within the U.S.

symantec™

I N D E X

F

H

I

J

K

L

M

N

O

P

Q

R

S